2007－ＤＳＭ－45（６）
2007／5／10

IPv6における複数アドレス選択技術の検討

藤崎 智宏　松本 存史†

†NTT 情報流通プラットフォーム研究所 〒180-8585 東京都武蔵野市緑町 3-9-11
E-mail: † fujisaki.tomohiro@lab.ntt.co.jp, arifumi@nttv6.net

あらまし マルチホーム環境など，複数の上流ネットワークに接続される IPv6 ネットワークには，アドレスプレフィックスが複数割り当てられることがある．このようなネットワークでは，同一リンク上に複数のアドレスプレフィックスが広告され，IPv6 ノードの単一インタフェースに複数の IPv6 アドレスが付与される．複数の IPv6 アドレスが付与されたホストが通信を開始する際には，始点アドレスの選択が必要となり，誤ったアドレスを選択すると通信が成立しない．本稿では，複数の IPv6 アドレスを持つホストにおける始点アドレス選択問題について検討し，解決手段として始点アドレス選択ポリシー配布機構を提案する．

キーワード IPv6，複数アドレス選択，マルチプレフィックス

Address Selection Mechanisms in a Multiple Address Network Environment

Tomohiro FUJISAKI† and Arifumi MATSUMOTO‡

†NTT Information Sharing Platform Laboratories 3-9-11 Midori-cho, Musashino-shi, Tokyo, 180-8585 Japan
E-mail: † fujisaki.tomohiro@lab.ntt.co.jp, arifumi@nttv6.net

Abstract An IPv6 network with multiple upstream networks has multiple IPv6 address prefixes, and a host in that network will be assigned multiple IPv6 addresses. In this case, when the node starts to communicate with another node, it has to select one proper source address. If wrong address is selected, the communication will fail because of the ingress filtering at upstream networks. This paper describes address selection problems and proposes a solution using address selection policy distribution mechanisms.

Keyword IPv6, Address selection, Multi-prefix

1. はじめに

近年，インターネットの利用が拡大し，利用目的の多様化が顕著である．従来は，別の手段で提供されていたアプリケーションが IP ネットワーク上で実現されることも増えてきている．例えば，IP 電話や映像配信は既に商用サービスとして提供されており，また，ビル・家庭などのファシリティ管理，防犯目的の遠隔監視なども IP ネットワーク上でのサービス検討が進んでいる．

このような多種多様のサービスを同時にユーザに提供する場合，複数の IP ネットワークをユーザ宅に引き込む，といった形態が考えられる．この形態において，サービス提供者が独自に IP アドレスを取得してネットワークを構築し，ユーザやユーザ宅内のサービス機器に直接アドレスを割り当てることで，サービス提供者が各種ポリシーを IP アドレスをベースとして実装することができる（1 サービス・1 プレフィックスモデル）．

現在のインターネットプロトコル（IPv4）の後継として標準化されたバージョン 6（IPv6）を利用することで，サービスごとのアドレス利用が可能となる．IPv6 は IPv4 に比較して広大なアドレス空間を有しており，個々の機器にまでグローバル IP アドレスを割り当てることが容易であるのみならず，個々のサービス提供者が独自のサービスを実現するためにアドレス空間を取得することも可能である．

ユーザ宅が複数のサービスネットワークに接続された場合，PC などの汎用デバイスは，同時に複数ネットワークに所属することがある．この場合，ネットワーク形態によっては，単一インタフェースに複数の IP アドレスが付与され，通信の際に，始点アドレスの選択が必要となる．

本稿では，IPv6 を利用して提供される複数のサービスを利用する場合に，複数のプレフィックスをユーザサイト内に引き込むマルチプレフィックス形態に着目し，その技術的課題と解決策について考察する。

2. マルチプレフィックスネットワーク

2.1. マルチプレフィックスネットワーク構築の利点

IP ネットワーク上で複数のサービスをユーザに直接提供する場合，単一の IP ネットワーク上にすべてのサービスを実装する方法と，サービスごとにネットワークを分離すること方法が考えられる．文献[1]では，後者のネットワーク形態をとることの利点として，

1．それぞれのユーザは，提供されているネットワークサービスをすべて同時に利用するわけではない．サービス提供者の観点からは，プロビジョニング等を考え，ユーザごとに提供するサービスを選択できた方がよい．
2．サービスごとに，パケットフィルタやネットワーク品質に関する考え方などの，ネットワークに対

する要求条件が異なる．サービスネットワークの管理者の観点からは，特にインターネット接続と別のネットワーク接続が利用できれば，アドレスベースの制御がしやすくなる．

といった点を挙げている．図1に，複数サービスをそれぞれ別のネットワークで提供している例を示す．

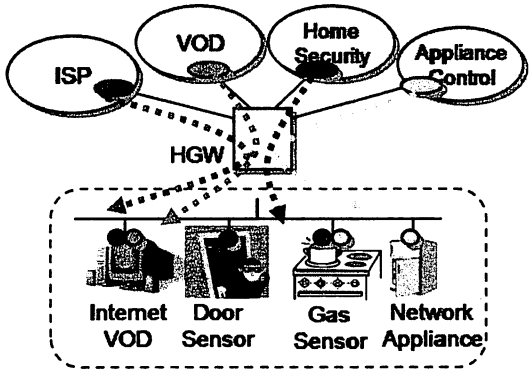

図1．マルチサービスネットワーク

この例では，ユーザは，インターネットサービス，ビデオオンデマンドサービス，ホームセキュリティサービス，ネットワーク家電制御サービスを利用しており，それぞれのサービスが別のネットワークによって提供されている．日本のコンシューマネットワークでは，このような環境は既に数多く存在し，IP電話，インターネット接続，および映像配信サービスが別ネットワークにて提供されている．現在のこれらのサービスは主に IPv4 を用いて実装されており，端末に割り振られる IPv4 アドレスは一つで，出口のホームゲートウェイ(HGW)で NAT を用いた始点アドレス変換を実施している．しかしながら，ユーザ数，端末数の増加による必要アドレス数を考慮すると，これらのサービスでも今後，IPv6 が利用されることになると考えられる．

2.2. IPv6 を利用したマルチプレフィックスネットワーク構築上の問題点

IPv6 の広大なアドレス空間を利用し，サービスごとに別々の IPv6 アドレスブロックを割り当てた場合，それぞれのサービスを利用する機器には個別の IPv6 アドレスが付与されるが，PC など複数のサービスを利用可能な機器には複数の IPv6 アドレスが付与されることになる．図1では，PC がインターネット接続サービスと VOD サービスを同時に利用しており，それぞれのサービスごとの IPv6 アドレスが付与されている例を示している．

端末が同一インタフェースに複数の IPv6 アドレスを持つ場合，通信を開始する際に通信相手に応じた正しい IPv6 アドレスを始点アドレスとして選択する必要がある．IPv6 の仕様では RFC3484[2]にて，複数アドレス選択のアルゴリズムを定義しているが，RFC3484 のディフォルトのアドレス選択ルールでは適切な始点アドレスの選択に失敗することがある．

3. RFC3484 のアドレス選択ルールに関する問題

本節では，RFC3484 で定義されているディフォルトのアドレス選択ルール適用の問題点を述べる．

3.1. 上流 ISP においてイングレスフィルタが存在する場合

ユーザサイトが複数の IPv6 ISP に接続しているネットワークを考える（図2）．この場合，ユーザサイトには上流 ISP それぞれからアドレスブロックが割り当てられ，端末には複数のアドレスが付与される．

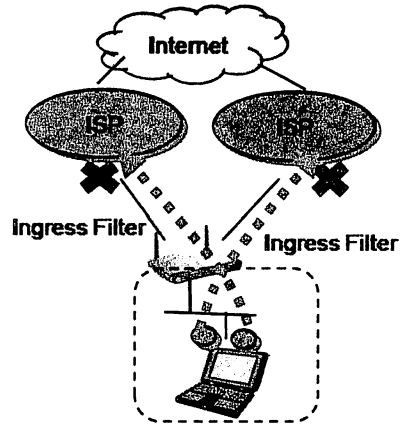

図2．複数 ISP との接続

このようなネットワーク環境で端末がパケットを送信する場合，通信の際に端末が選択した始点アドレスが，パケットが送信される上流 ISP が割り当てたものでないことがある．昨今，セキュリティ対策としてアドレス詐称を防ぐために，ユーザから送信されるパケットについて，自ネットワークのアドレス以外をフィルタすることが一般的になってきている[3]．このため，選択された始点アドレスによっては，パケットが届かない，といった事象が発生する．特に，コンシューマネットワークのような比較的小規模なサイトの場合，ISP は経路情報を提供せず，ディフォルトルートを利用した経路制御を実施している場合が多い．この場合，ディフォルト経路が向いている ISP から割り当てられた IPv6 アドレス以外を始点アドレスとして用いたパケットは，フィルタされてしまう．

3.2. 閉域ネットワークとインターネットの同時接続

閉域ネットワークとインターネットに同時接続されたサイトでは，始点アドレス選択が大きな問題になる．図3に，閉域ネットワークと ISP に同時に接続されたサイトの例を示す．この例では，ユーザサイトに ISP と閉域ネットワークからそれぞれ IPv6 アドレスブロックが割り当てられ，端末には二つの IPv6 アドレスが付与されている．

RFC3484 では，始点アドレス選択のディフォルトルールとして，アドレスを選択する際，終点アドレスとのロンゲストマッチを用いる．図3の例では，通信相手であるイン

ターネット上の端末の持つ IPv6 アドレスとマッチするアドレスは，閉域ネットワークから付与されたアドレスであり，ISP がフィルタを実施していなかったとしても戻りの経路がないため通信が成立しない．

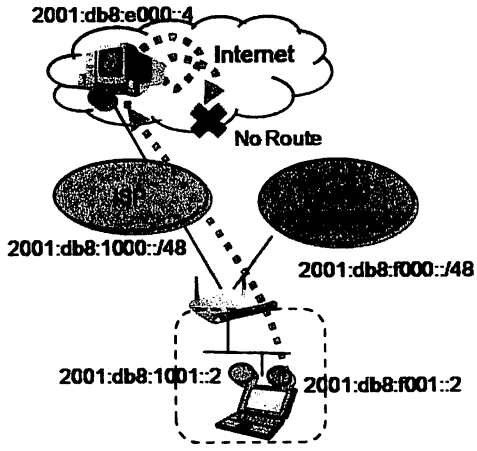

図３．閉域ネットワークと ISP の同時接続

3.3. グローバル IPv6 アドレスと ULA との併用

文献[4]では，ユニークローカル IPv6 ユニキャストアドレス（ULA[5]）[1]を用いて，NAT が存在しない IPv6 ネットワーク環境において IPv4 の NAT と同等のセキュリティを担保する仕組みについて述べている．

インターネットとの通信が必要ないネットワークプリンタのような機器には ULA のみを付与し，インターネットと通信する PC に等はグローバルアドレスと ULA の双方を付与することでネットワークセキュリティの担保が図れる（図４）．

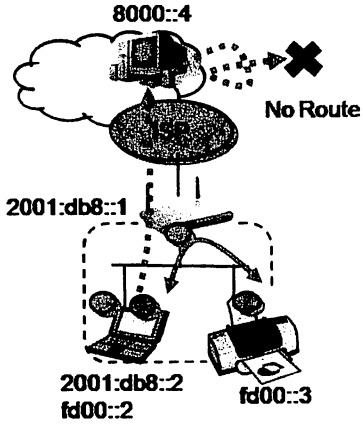

図４．ULA とグローバルアドレスの併用

[1] IPv6 における IPv4 プライベートアドレス(RFC1918)相当のアドレス．

この例では，RFC3484 のロンゲストマッチルールに従い，ULA アドレス宛に通信をする場合のみ ULA アドレスが選択される．しかしながら，IPv6 の利用が進み，トップビットが 1 になった IPv6 アドレスの配布が開始された場合，そのようなアドレスを持つサーバ（図４の 8000::4 等）への通信の際に ULA が選択されてしまい，通信が成立しないことになる．

3.4. IPv4 と ULA の同時利用

IPv4 ネットワークに，外部接続性のない ULA 等の IPv6 アドレスを利用した IPv6 ネットワークを重畳させた場合に，終点アドレスの選択問題が発生する．図５に問題となるネットワークの例を示す．

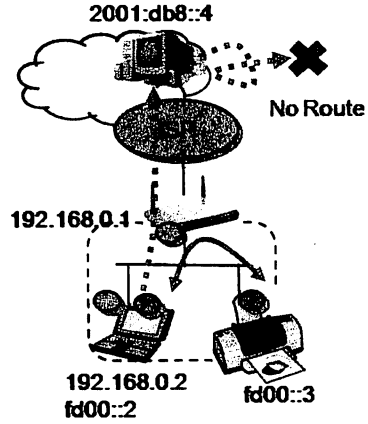

図５．IPv4 アドレスと ULA との併用

RFC3484 のディフォルト規則では，通信相手が IPv4 アドレスと IPv6 アドレスを持っていた場合，IPv4 による通信よりも，IPv6 による通信を優先する．このため，インターネット上の IPv4/IPv6 両方のアドレスを持つサイト（デュアルスタックサイト）にアクセスする際，端末に IPv4 アドレスと IPv6 アドレスの両方が付与されている場合には，IPv6 による通信を先に実施する．ULA のみを利用したネットワークなどで IPv6 接続に問題があった場合には通信に失敗することになる．

4.5. アドレス選択に関するその他の要求

上記以外にも，アドレス選択に対する要求として，以下のような点が考えられる．

- IPv6 プライバシーアドレス[6]の使用の制御
  IPv6 のステートレスアドレス自動設定では，ネットワークインタフェースの MAC アドレスから導出したアドレスが利用されることが多いため，プライバシーの問題が指摘されていた．RFC3041 では，ランダムにアドレスを生成することで，プライバシーの隠蔽を図る機構を定義しているが，この機構の利用を管理者が制御したいことがある．
- IPv4 と IPv6 共存
  管理者が，通信の際に IPv4 通信を優先するか IPv6 通信を優先するかを制御することで，IPv4 ネット

ワークと IPv6 ネットワークの共存が図れる.

- ネットワークアドレス付け替えのサポート
  ネットワークのアドレスを付け替える際，管理者が新アドレスと旧アドレスの利用を制御することができれば，スムーズなアドレス付け替えが実施できる.

5. アドレス選択問題解決のアプローチ

本節では，アドレス選択問題解決に関する取り組みについて述べる．アドレス選択問題の解決案としては，プロアクティブアプローチと，リアクティブアプローチが考えられる.

プロアクティブアプローチ

通信を実施する前に，必要な情報をノードに提供するアプローチである．このアプローチの例としては，

1. アドレス選択に必要な情報をノードに事前に配布するアドレス選択ポリシー配布機構. 次章で詳述する.
2. 通信の際に相手のアドレスに対応する始点アドレスに対する情報を外部のサーバ等に問い合わせ，始点アドレスを選択する方法. 通信の宛先ノードへの経路情報は，サイトのルーティングシステムが保有しているため，ルーティングシステムとの情報のやりとりを実施し，対応する始点アドレスを決定する.

等が考えられる.

リアクティブアプローチ

通信を実行し，ICMP エラーやタイムアウトなど，ネットワークからの応答を元にアドレス選択を再度実施するアプローチである．リアクティブアプローチとしては，

3. 文献[9]で提案されているような，IP 層でパケットをキャッシュし，ICMP エラー等が帰ってきた場合には始点アドレスを変更して再送するような機
4. shim6[10] として標準化が進んでいる，IP 層とトランスポート層の間に shim 層を新たに設け，IP 層でのアドレス変更を上位層には隠蔽することで複数アドレスの動的な切り替えをサポートする機

等が考えられる.

上記は，1 がもっとも静的であり，4 がもっとも動的なアプローチとなっている.

6. アドレス選択ポリシー配布機構

[1]にも述べられているように，RFC3484 で定義されている IPv6 アドレス選択ポリシーを端末に配布し，利用することで複数アドレスの選択を制御することが可能となる．筆者らは，このアドレスポリシー配布機構を提案している[7]. 本提案では，"Default Address Selection Policy Option." という新しい DHCPv6 オプションを定義し，IPv6 環境でプロバイダからユーザにアドレスブロックを割り当てるプロトコルである DHCP-PD に重畳してアドレス選択ポリシーを配布する．サイト内では，DNS サーバアドレス等を配布する DHCPv6 を利用し，各端末まで選択ポリシーが配布される．RFC3484 で定義されているアドレス選択ポリシー機構はすでに多くのオペレーティングシステムで実装されているため[8]，端末へのアドレスポリシー配布機構を規定することで，管理者によるアドレス選択の制御が可能となる．図 6 に配布機構の動作を示す.

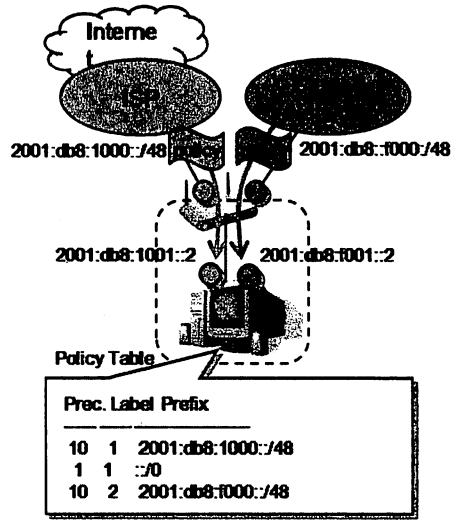

図 6．アドレス選択ポリシー配布

ネットワーク環境は，図 3 で示したものと同一である．ISP と閉域ネットワークより，アドレスブロックとあわせ，アドレス選択に関するポリシーを配布する．ユーザサイトのルータでは，配布されたポリシーをマージした上で，宅内の機器に配信する．この選択ポリシーテーブルを利用することで，通信相手のアドレスに応じた始点アドレスが選択される.

6.1. アドレス選択ポリシー配布機構の実装

[7]で提案しているポリシー配布プロトコルを実装した.

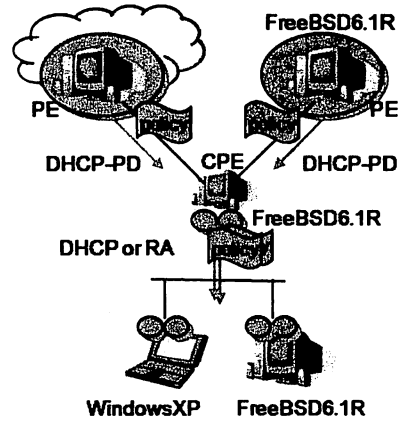

図 7．アドレス選択ポリシー配布実証システム

[11]にて提供されている DHCPv6 サーバを拡張し，

Default Address Selection Policy Option を実装した．また，[12]の DHCPv6 クライアントを拡張し，同時に Windows XP 上に移植した．また，クライアント端末上で，取得したアドレス選択ポリシーを OS のアドレス選択ポリシーテーブルに設定するプログラムも実装した．

作成した実装を，プロバイダ環境を模擬した図 7 に示すネットワーク構成において動作させた．PE，および CPE としては FreeBSD 6.1Release を，クライアントとしては FreeBSD 6.1Release と Windows XP を使用した．

図 7 の環境で，PE から DHCP-PD によって配布したアドレス選択ポリシーが CPE を経由し，ユーザ宅内端末である Windows XP 機器，FreeBSD 機器に配信されていること，および，配信されたポリシーが OS のポリシーテーブルに設定され，設定された情報に基づき始点アドレス選択が実施されていることを確認した．

6.2. 実ネットワークにおける複数アドレス選択の実際

当研究所では，2005 年 6 月よりマルチプレフィックス環境の運用を実施している．ネットワークの概略構成を図 8 に示す．

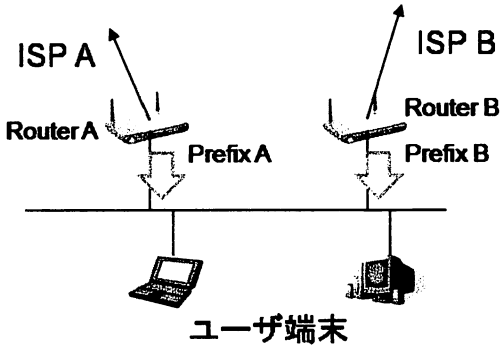

図 8．社内 IPv6 実験ネットワーク

本実験ネットワークは，複数の上流 IPv6 ISP と接続しており，それぞれ別々の IPv6 アドレスプレフィックスが割り当てられている．実験セグメントにおいては，それぞれの上流 ISP ごとに別々のルータを設置し，それぞれ，上流 ISP から取得したアドレスブロックのネットワークプレフィックスを広告している．同ネットワークには，常時 20 台 IPv6 対応機器が存在している．このネットワーク環境では，接続されているユーザ端末は複数の IPv6 アドレスプレフィックスと，複数のディフォルトルータを持つ．

この環境で，それぞれのルータに到着する，自プレフィックス，および別プレフィックスのパケット数を測定した．測定結果を表 1 に示す．

	パケット種別	パケット数 (Packets/day)
Router A	Prefix A	25,000
	Prefix B	26,000
Router B	Prefix A	3,500
	Prefix B	37,000

表 1．ルータに到着したパケット数

IPv6 の仕様では，複数のルータが存在する場合に，どのルータが選択されるかは実装依存である．また，始点アドレスとして選択されるプレフィックスは通信相手によって決まるため，複数のユーザが利用しているネットワークにおいて，選択されるプレフィックスの割合を予測することは困難である．しかしながら，測定結果から，Router A に到着するほぼ半分のパケットが別プレフィックスのものであり，このパケット（表 1 中，網掛け部分のパケット）はイングレスフィルタ等で遮断される可能性のあるものである．当該ネットワーク中のノードすべてが RFC3484 のアドレス選択ポリシーによる制御機構を実装しているわけではないが，アドレス選択ポリシー配布機構を導入することで，これらのパケットを減少させることが期待できる．

7. まとめ

本稿では，ノードに複数の IPv6 アドレスが付与される場合に発生する問題を提起し，その解決案として始点アドレス選択ポリシー配布機構を提案した．今後，IPv6 ネットワークが広まるにつれ，複数の IPv6 プレフィックスが割り当てられるネットワークが増加する．提案手法を用いることで，始点アドレス選択の制御が可能になる．

文　献

[1] SUZUKI Shinsuke, ``Providing Network Services with Multiple Prefix Delegation", SAINT 2004 Workshop

[2] R. Draves, ``Default Address Selection for Internet Protocol version 6 (IPv6)," RFC 3484, Feb 2003

[3] Ferguson, P. and D. Senie, "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing", BCP 38, RFC 2827, May 2000.

[4] G. Van de Velde, T. Hain, R. Droms, B. Carpenter, E. Klein, ``Local Network Protection for IPv6," <draft-ietf-v6ops-nap-06.txt>, Internet-Draft, Jan 2007.

[5] R. Hinden, B. Haberman, `` Unique Local IPv6 Unicast Addresses," RFC 4193, Oct 2005.

[6] T. Narten, R. Draves, `` Privacy Extensions for Stateless Address Autoconfiguration in IPv6," RFC 3041, Jan. 2001.

[7] T. Fujisaki, A. Matsumoto, S. Niinobe, ``Distributing Default Address Selection Policy using DHCPv6," <draft-fujisaki-dhc-addr-select-opt-03.txt>, Internet-Draft, Jan. 2007.

[8] "Summary and Status of Default Address Selection for IPv6", http://www.nttv6.net/dass/

[9] M.Bagnulo "Updating RFC 3484 for multihoming support",<draft-bagnulo-ipv6-rfc3484-update-00.txt>, Internet-Draft, Dec 2005

[10] Shim6, http://www.ietf.org/html.charters/shim6

[11] http://www.wide-dhcpv6.sourceforge.net/

[12] KAME Project http://www.kame.net/